

From the Physics to the Computational Complexity of Multiboson Correlation Interference

Simon Laibacher and Vincenzo Tamma*

*Institut für Quantenphysik and Center for Integrated Quantum Science
and Technology (IQST), Universität Ulm, D-89069 Ulm, Germany*

We demonstrate how the physics of *multiboson correlation interference* leads to the computational complexity of linear optical interferometers based on correlation measurements in the degrees of freedom of the input bosons. In particular, we address the task of *MultiBoson Correlation Sampling* (MBCS) from the probability distribution associated with polarization- and time-resolved detections at the output of random linear optical networks. We show that the MBCS problem is fundamentally hard to solve classically even for nonidentical input photons, regardless of the color of the photons, making it also very appealing from an experimental point of view. These results fully manifest the quantum computational supremacy inherent to the fundamental nature of quantum interference.

Motivation. The interference of multiple bosons based on high-order correlation measurements [1–3] in a linear network is a phenomenon that is fundamental in atomic, molecular, and optical physics. The richness of its features gives rise to a wide variety of applications in quantum information processing [1, 4, 5], quantum metrology [6–8], and imaging [9]. Already correlated detections of two bosons after the interaction with a balanced beam splitter reveal an interference effect of truly quantum mechanical origin [10–13]: both particles always end up in the same output port due to the destructive interference of the two-boson quantum paths in which the bosons are either both reflected or both transmitted.

Going to higher-order correlation measurements in optical networks of large dimensions, multiboson interference becomes increasingly complex, promising a computational power that is not achievable classically [14, 15]. Multiphoton correlation experiments with more than two photons have already been performed [16–26], providing an important milestone towards experiments of higher orders [27, 28].

These experiments are usually based on joint measurements at the interferometer output ports “classically” averaging over the photons’ degrees of freedom (e.g. time, polarization). In this context, Aaronson and Arkhipov argued the computational hardness of multiboson interference in linear optics for identical bosons by introducing the well-known boson sampling problem [14]. Does this computational hardness also occur for nonidentical photons? While the computational complexity for partially distinguishable photons is still not known [15], it is clear that boson sampling becomes computationally trivial for fully distinguishable photons when the information about the detection times and polarizations is completely ignored.

However, recent technological advances have enabled experimentalists to produce arbitrarily polarized single photons with near arbitrary spectral and temporal properties [29–31] which can be “read out” by time- and

polarization-resolving measurements [1, 32–35] with extremely fast detectors [36]. This makes it possible to encode entire “quantum alphabets” in the degrees of freedom of multiple photons [37, 38] and to retrieve the encoded information by correlation measurements in those degrees of freedom, representing a valuable tool in quantum information processing [1, 39–52].

All these remarkable technological achievements now allow experimentalists to fully address the following fundamental questions about the interplay between the physics and the complexity of multiboson interference: How do the spectral distributions of N nonidentical photons determine the occurrence of N -photon interference events in time- and polarization-resolving correlated measurements? How and to what degree is this occurrence connected with computational complexity? Does computational hardness really disappear for input bosons that are completely distinguishable in their spectra? This letter aims to answer all these important questions, from both a fundamental and an experimental point of view, demonstrating the inherent computational complexity of the physics of multiboson correlation interference even for nonidentical photons.

MultiBoson Correlation Sampling (MBCS).

We consider N single photons prepared at the N input ports of a linear interferometer (see Fig. 1) with $2M \gg 2N$ ports. The interferometer unitary transformation \mathcal{U} is chosen randomly according to the Haar measure and is implemented by using a polynomial number (in M) of passive linear optical elements [53]. The state of N single photons injected in a set \mathcal{S} of N input ports $s \in \mathcal{S}$ is given by

$$|\mathcal{S}\rangle := \bigotimes_{s \in \mathcal{S}} |1[\xi_s]\rangle_s \bigotimes_{s \notin \mathcal{S}} |0\rangle_s,$$

with the single photon states

$$|1[\xi_s]\rangle_s := \sum_{\lambda=1,2} \int_0^\infty d\omega (\mathbf{e}_\lambda \cdot \boldsymbol{\xi}_s(\omega)) \hat{a}_{s,\lambda}^\dagger(\omega) |0\rangle_s, \quad (1)$$

where $\{\mathbf{e}_1, \mathbf{e}_2\}$ is an arbitrary polarization basis and $\hat{a}_{s,\lambda}^\dagger(\omega)$ is the creation operator for the frequency mode

* vincenzo.tamma@uni-ulm.de

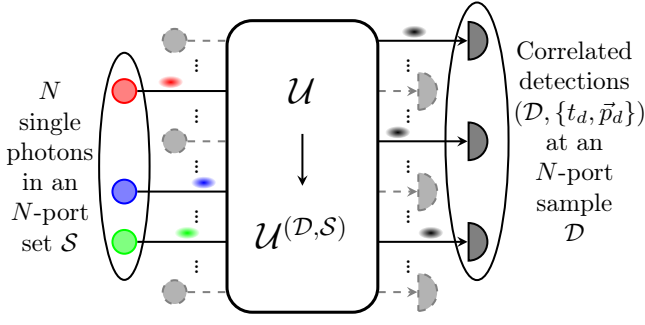


FIG. 1. General setup for multiboson correlation sampling. N single photons are injected into an N -port subset \mathcal{S} of the $M \gg N$ input ports of a random linear interferometer. At the output of the interferometer, they are detected in one of the possible port samples \mathcal{D} containing N of the M output ports at corresponding detection times and polarizations $\{t_d, \mathbf{p}_d\}_{d \in \mathcal{D}}$. For each output port sample \mathcal{D} and given input configuration \mathcal{S} , the evolution through the interferometer is fully described by a $N \times N$ submatrix $\mathcal{U}^{(\mathcal{D}, \mathcal{S})}$ of the $M \times M$ interferometer matrix \mathcal{U} .

ω and the polarization λ [54]. The complex spectral amplitude

$$\xi_s(\omega) := \mathbf{v}_s \xi_s(\omega - \omega_s) e^{i\omega t_{0s}} \quad (2)$$

is defined by the spectral shape $\xi_s(\omega - \omega_s) \in \mathbb{R}$ (centered around the central frequency (photon color) ω_s and with normalization $\int d\omega |\xi_s(\omega)|^2 = 1$), the polarization \mathbf{v}_s , and the time t_{0s} of emission of the photon injected in the port $s \in \mathcal{S}$. For simplicity, we consider input-photon spectra satisfying the narrow bandwidth approximation and a polarization-independent interferometric evolution with equal propagation time Δt for each possible path from an input source to a detector at the interferometer output.

Given such a multiboson interferometer and assuming identical photons, $\xi_s = \xi \forall s \in \mathcal{S}$, the boson sampling problem [14] was defined by Aaronson and Arkhipov as the task of sampling from the probability distribution over the output port samples \mathcal{D} , regardless of detection times and polarizations. We address here an interesting generalization of this famous problem by introducing the problem of MultiBoson Correlation Sampling (MBCS) [1, 55]. The MBCS problem is defined as the task of sampling at the interferometer output from the probability distribution associated with time- and polarization-resolving correlation measurements. Each possible sample corresponds to an N -photon detection event at an N -port subset \mathcal{D} of the M output ports at given times and polarizations $\{t_d, \mathbf{p}_d\}_{d \in \mathcal{D}}$, with $\mathbf{p}_d \in \{\mathbf{e}_1, \mathbf{e}_2\}$ [56]. The N -photon detection probability rate corresponding to a sample $(\mathcal{D}, \{t_d, \mathbf{p}_d\}_{d \in \mathcal{D}})$ depends [1] on both the $N \times N$ submatrix

$$\mathcal{U}^{(\mathcal{D}, \mathcal{S})} := [\mathcal{U}_{d,s}]_{\substack{d \in \mathcal{D} \\ s \in \mathcal{S}}}$$

of the $M \times M$ unitary matrix \mathcal{U} describing the interferometer, and the Fourier transforms

$$\begin{aligned} \chi_s(t) &:= \mathcal{F}[\xi_s](t - \Delta t) \\ &= \mathbf{v}_s \chi_s(t - t_{0s} - \Delta t) e^{i\omega_s(t - t_{0s} - \Delta t)} \end{aligned} \quad (3)$$

of the single-photon spectra $\xi_s(\omega)$ in Eq. (2) (with $\chi_s(t)$ being the Fourier transform of $\xi_s(\omega)$). Defining the matrices

$$\mathcal{T}_{\{t_d, \mathbf{p}_d\}}^{(\mathcal{D}, \mathcal{S})} := [\mathcal{U}_{d,s} (\mathbf{p}_d \cdot \chi_s(t_d))]_{\substack{d \in \mathcal{D} \\ s \in \mathcal{S}}}$$

and using the definition

$$\text{perm } \mathcal{M} := \sum_{\sigma \in \Sigma_N} \prod_{i=1}^N \mathcal{M}_{i, \sigma(i)}$$

of the permanent of a matrix \mathcal{M} , where the sum runs over all permutations σ in the symmetric group Σ_N , the probability rate of an N -fold detection event $(\mathcal{D}, \{t_d, \mathbf{p}_d\}_{d \in \mathcal{D}})$ is

$$G_{\{t_d, \mathbf{p}_d\}}^{(\mathcal{D}, \mathcal{S})} = \left| \text{perm } \mathcal{T}_{\{t_d, \mathbf{p}_d\}}^{(\mathcal{D}, \mathcal{S})} \right|^2, \quad (4)$$

for ideal photodetectors.

By considering an integration time T_I short enough such that

$$\begin{aligned} \forall t_d : \chi_s(t - t_{0s} - \Delta t) \chi_{s'}(t - t_{0s'} - \Delta t) e^{i(\omega_s - \omega_{s'})t} &\approx \text{const.} \\ \forall t \in [t_d - T_I, t_d + T_I], \forall s, s' \in \mathcal{S}, \end{aligned} \quad (5)$$

we obtain, for a detection sample $(\mathcal{D}, \{t_d, \mathbf{p}_d\}_{d \in \mathcal{D}})$, the probability

$$P_{\{t_d, \mathbf{p}_d\}}^{(\mathcal{D}, \mathcal{S})} = (2T_I)^N \left| \text{perm } \mathcal{T}_{\{t_d, \mathbf{p}_d\}}^{(\mathcal{D}, \mathcal{S})} \right|^2 \quad (6)$$

of an N -fold detection in the time intervals $\{[t_d - T_I, t_d + T_I]\}_{d \in \mathcal{D}}$, where the detection time axes are discretized with step width $2T_I$.

We emphasize that, for each possible sample $(\mathcal{D}, \{t_d, \mathbf{p}_d\}_{d \in \mathcal{D}})$, the probability in Eq. (6) is at most exponentially small in N , as demonstrated in Theorem 1 in the Supplemental Material [57].

Exact MBCS. Obviously, the complexity of sampling exactly from the probability distribution defined by Eq. (6) depends on the N -tuples $\{\xi_s\}_{s \in \mathcal{S}}$ of single-photon input spectra in Eq. (2) [58].

With that in mind, in order to establish the complexity of exact MBCS, it is useful to define the N -photon interference matrix with elements

$$a(s, s') := |\mathbf{v}_s \cdot \mathbf{v}_{s'}| \int_{-\infty}^{\infty} dt |\chi_s(t - t_{0s})| |\chi_{s'}(t - t_{0s'})| \leq 1, \quad (7)$$

with $s, s' \in \mathcal{S}$, depending on the pairwise overlaps of the absolute values of the temporal single-photon detection

amplitudes [59] $\chi_s(t - t_{0s} - \Delta t) e^{i\omega_s(t - t_{0s} - \Delta t)}$ and of the polarizations \mathbf{v}_s in Eq. (3). For non-vanishing elements

$$0 < a(s, s') \leq 1 \quad \forall s, s' \in \mathcal{S}, \quad (8)$$

there exists a time interval T and at least a polarization $\mathbf{e}_{\bar{\lambda}} \in \{\mathbf{e}_1, \mathbf{e}_2\}$, such that

$$\mathbf{e}_{\bar{\lambda}} \cdot \boldsymbol{\chi}_s(t_d) \neq 0 \quad \forall t_d \in T, \forall s \in \mathcal{S}, \forall d \in \mathcal{D}.$$

It is then ensured that for each detection sample $(\mathcal{D}, \{t_d, \mathbf{p}_d\}_{d \in \mathcal{D}})$, with $t_d \in T, \mathbf{p}_d = \mathbf{e}_{\bar{\lambda}} \forall d \in \mathcal{D}$, the input photons are indistinguishable at the detectors: this leads to the interference of all possible $N!$ N -photon quantum paths manifested by the coherent superposition of all corresponding, non-vanishing $N!$ N -photon detection amplitudes in Eq. (4). Therefore, only the conditions (5) and (8) for the nonidentical input spectra $\{\boldsymbol{\xi}_s\}_{s \in \mathcal{S}}$ in Eq. (2) are enough to ensure the occurrence of N -photon correlation interference events.

Even more interestingly, the same simple conditions lead to the computational hardness of the exact MBCS problem, establishing a connection between the occurrence of multiphoton correlation interference and complexity. Indeed, for approximately equal detection times $t_d \approx t \in T$ and equal polarizations $\mathbf{p}_d = \mathbf{e}_{\bar{\lambda}}, \forall d \in \mathcal{D}$, the multiphoton detection probabilities in Eq. (6) become

$$P_{\{t_d, \mathbf{p}_d\}}^{(\mathcal{D}, \mathcal{S})} = \left| \text{perm} \mathcal{U}^{(\mathcal{D}, \mathcal{S})} \right|^2 (2T_I)^N \prod_{s \in \mathcal{S}} |\mathbf{e}_{\bar{\lambda}} \cdot \boldsymbol{\chi}_s(t)|^2. \quad (9)$$

The interference of all N -photon quantum paths in Eq. (9) depends, apart from an overall factor, only on the permanent of a submatrix $\mathcal{U}^{(\mathcal{D}, \mathcal{S})}$ of the interferometer random unitary matrix \mathcal{U} . For $N \ll M$, these matrices have elements given by approximately independent and identically distributed (i.i.d.) Gaussian random variables and the approximation of their respective permanents is a #P-hard task [14]. We emphasize that the presence of only an arbitrarily small fraction of samples with probabilities as in Eq. (9) would be enough to ensure the hardness of the exact MBCS. This can be shown analogously to the hardness proof of the original problem of exact boson sampling in [14]. Indeed, the ability to perform exact MBCS with a polynomial number of resources would imply that the task of approximating any given, fixed permanent associated with the probability distribution (6) is in the complexity class BPP^{NP}. Since this would also include the task of approximating the #P-hard permanents emerging in Eq. (9), the polynomial hierarchy would collapse to the third level, which is strongly believed to be highly unlikely. We refer to section II of the Supplemental Material for more details [57].

Interestingly, differently from the original boson sampling problem [14], the classical intractability of exact MBCS is not conditioned on input photons with approximately identical spectra $\boldsymbol{\xi}_s$ in Eq. (2). Only the simple conditions (5) and (8) on the spectra are enough to guarantee its computational hardness.

Approximate MBCS. Is approximate MBCS also not tractable with a classical computer? Such a question is obviously of fundamental importance from an experimental point of view, since it takes into account the inevitable experimental errors in an MBCS quantum interferometer which make only approximate sampling possible [58]. We consider, for simplicity, the case of an N -photon interference matrix in Eq. (7) with unit elements

$$a(s, s') \cong 1 \quad \forall s, s' \in \mathcal{S}. \quad (10)$$

This corresponds to two possible scenarios. Either all the input photons are completely identical or they differ only by their color, i.e. central frequency. In these cases the input photons have equal polarizations and are always indistinguishable at the detectors independently of the detection times and polarizations.

To simplify the expressions, we consider here polarization-insensitive detectors.

a. Identical input photons. For approximately identical frequency spectra

$$\boldsymbol{\xi}_s(\omega) \cong \boldsymbol{\xi}(\omega) \quad \forall s \in \mathcal{S},$$

by using Eq. (6), the polarization-insensitive detection probability reads

$$\begin{aligned} P_{\{t_d\}}^{(\mathcal{D}, \mathcal{S})} &:= \sum_{\{\mathbf{p}_d\} \in \{\mathbf{e}_1, \mathbf{e}_2\}^N} P_{\{t_d, \mathbf{p}_d\}}^{(\mathcal{D}, \mathcal{S})} \\ &= \left| \text{perm} \mathcal{U}^{(\mathcal{D}, \mathcal{S})} \right|^2 (2T_I)^N \prod_{d \in \mathcal{D}} |\boldsymbol{\chi}(t_d)|^2, \end{aligned}$$

where we used the property $\sum_{\mathbf{p}_d = \mathbf{e}_1, \mathbf{e}_2} |\mathbf{p}_d \cdot \mathbf{v}| = |\mathbf{v}|^2 = 1$. Of course the only possible events occur within a detection-time interval where the function $|\boldsymbol{\chi}(t_d)| = |\mathcal{F}[\boldsymbol{\xi}](t_d - \Delta t)|$ is not negligible. Here, independently of the detection times $\{t_d\}_{d \in \mathcal{D}}$, all the probability rates associated with each possible sample $(\mathcal{D}, \{t_d\}_{d \in \mathcal{D}})$ are given, apart from a prefactor, by the permanents of $N \times N$ submatrices $\mathcal{U}^{(\mathcal{D}, \mathcal{S})}$ of the interferometer transformation \mathcal{U} .

When the observer ignores the information about the detection times the approximate MBCS problem reduces to the well known standard formulation of the approximate boson sampling problem, which Aaronson and Arkhipov argued to be intractable with a classical computer [14]. Therefore, the approximate MBCS problem is at least as complex as the original approximate boson sampling problem.

b. Photons of different colors. We now address the case of input photons in Eq. (1) with spectral distributions

$$\boldsymbol{\xi}_s(\omega) = \mathbf{v} \xi(\omega - \omega_s) e^{i\omega t_0},$$

with equal emission times $t_{0s} = t_0$ and equal polarizations $\mathbf{v}_s = \mathbf{v}$ but different colors ω_s . For simplicity, we consider spectral shapes

$$\xi(\omega) = \frac{1}{\sqrt{\pi\Delta\omega}} \text{sinc}\left(\frac{\omega}{\Delta\omega}\right)$$

with equal bandwidths $\Delta\omega_s = \Delta\omega \lesssim |\omega_s - \omega_{s'}| \ \forall s, s'$, where $\text{sinc } x := \sin x/x$. The N -photon interference at the detectors is therefore characterized by the Fourier transforms

$$\chi_s(t) = v \sqrt{\frac{\Delta\omega}{2}} \text{rect} \left(\frac{\Delta\omega(t - t_0 - \Delta t)}{2} \right) e^{i\omega_s(t - t_0 - \Delta t)},$$

with the rectangular function

$$\text{rect } x := \begin{cases} 1 & |x| < \frac{1}{2} \\ \frac{1}{2} & |x| = \frac{1}{2} \\ 0 & \text{else} \end{cases}.$$

Therefore, the condition (10) is satisfied, and the probability rates in Eq. (4) are non-vanishing only for detection times $t_d \in T := [t_0 + \Delta t - 1/\Delta\omega, t_0 + \Delta t + 1/\Delta\omega] \ \forall d \in \mathcal{D}$. Moreover, Eq. (5) is fulfilled for integration times

$$T_I \ll |\omega_s - \omega_{s'}|^{-1} \ \forall s, s' \in \mathcal{S}, \quad (11)$$

where $(T_I \Delta\omega)^{-1}$ defines the number of discrete steps of length $2T_I$ along the time interval T . As is known, detectors with such high time-resolution cannot distinguish photons of different colors ω_s and multiphoton interference can be observed. Indeed, from Eq. (6), the polarization-independent detection probabilities are

$$P_{\{t_d\}}^{(\mathcal{D}, \mathcal{S})} = (\Delta\omega T_I)^N \left| \text{perm} \left([\mathcal{U}_{d,s}^{(\mathcal{D}, \mathcal{S})} e^{i\omega_s t_d}]_{\substack{d \in \mathcal{D} \\ s \in \mathcal{S}}} \right) \right|^2 \quad (12)$$

for all possible detection time intervals $[t_d - T_I, t_d + T_I] \subset T$. Such probabilities are proportional to permanents of matrices whose elements are the elements of $\mathcal{U}^{(\mathcal{D}, \mathcal{S})}$ multiplied by the complex phases $\exp(i\omega_s t_d)$.

Since the elements $\mathcal{U}_{d,s}^{(\mathcal{D}, \mathcal{S})}$ of the submatrices $\mathcal{U}^{(\mathcal{D}, \mathcal{S})}$ are i.i.d. Gaussian random variables and the phase factors $e^{i\omega_s t_d}$ only rotate such elements in the complex plane, the entries of the matrices $[\mathcal{U}_{d,s}^{(\mathcal{D}, \mathcal{S})} e^{i\omega_s t_d}]_{\substack{d \in \mathcal{D} \\ s \in \mathcal{S}}}$ are also i.i.d. Gaussian random variables as shown in App. C of the Supplemental Material [57]. Therefore, the probability distribution of the interferometer output interestingly depends, for all possible samples, on permanents whose approximation to within a multiplicative factor is a #P-hard problem [14]. Consequently, even for input photons of different colors, it is possible to show in analogy with Ref. [14] that approximate MBCS is of at least the same complexity as the standard boson sampling with identical photons [60]. As a “bonus”, the number of possible samples $(\mathcal{D}, \{t_d\}_{d \in \mathcal{D}})$ is exponentially larger (by a factor $(T_I \Delta\omega)^{-N}$ with $T_I \Delta\omega \ll 1$ according to Eq. (11)) with respect to the standard boson sampling problem.

Does approximate MBCS retain its complexity even for photons which are completely pairwise distinguishable in their colors ω_s (i.e. $\omega_s - \omega_{s'} \gg \Delta\omega \ \forall s \neq s'$)? We first

emphasize that, since these photons are characterized by a pairwise overlap

$$\int_0^\infty d\omega \xi_s(\omega) \cdot \xi_{s'}(\omega) \cong 0 \quad \forall s \neq s', \quad (13)$$

the approximate boson sampling problem is trivial [14]. Indeed, in this case, by averaging the rate in Eq. (4) over all possible detection times and polarizations, one finds that the boson sampling probability [1]

$$P^{(\mathcal{D}, \mathcal{S})} = \text{perm} [|\mathcal{U}_{d,s}^{(\mathcal{D}, \mathcal{S})}|^2]_{\substack{d \in \mathcal{D} \\ s \in \mathcal{S}}},$$

for an output port sample \mathcal{D} , is given by the permanent of a non-negative matrix that can be approximated with a polynomial number of resources [61]. Consequently, one might guess that also the approximate MBCS is computationally trivial. Nonetheless, the complexity emerging from the result in Eq. (12) is independent of the colors ω_s of the input photons, demonstrating that also in this case approximate MBCS is classically intractable.

Two essential physical aspects are behind the demonstrated complexity of approximate MBCS: *all* possible detection-time events can be an outcome of the sampling experiment (none of the events is disregarded) and *all* these time samples arise from the interference of $N!$ multiphoton quantum paths. In conclusion, the physics of sampling among all possible N -photon interference events behind our proposal is at the heart of the complexity of approximate MBCS.

Discussion. In this letter, we demonstrated how and to what degree the occurrence of multiphoton interference in time- and polarization-resolving correlation measurements leads to computational hardness in linear optical interferometers.

The definition of an N -photon interference matrix $a(s, s')$ in Eq. (7) allowed us to formulate the simple sufficient condition (8) on the spectra of the input photons for the occurrence of N -photon interference, provided sufficiently small integration times (see Eq. (5)).

Remarkably, these two simple conditions are also sufficient to guarantee the complexity of exact MBCS. In contrast, the complexity of the original exact boson sampling problem has only been proven for identical input photons.

For approximate MBCS on the other hand, not only the existence of samples exhibiting full N -photon interference (guaranteed by (8)) is important but also their fraction with respect to the total number of samples. Interestingly, this is encoded in the magnitude of the entries $a(s, s')$ of the N -photon interference matrix in Eq. (7).

It was thus natural to consider the simple case of full overlap of the modulus of the single-photon detection amplitudes ($a(s, s') = 1$) where all possible detection events correspond to N -photon interference samples [62]. In this case, corresponding to identical input photons or photons with arbitrary colors, approximate MBCS is at least of

the same complexity as boson sampling with identical photons.

This is particularly interesting if the differences in the central frequencies are much larger than the width of the single photons' spectral shapes, corresponding to fully distinguishable photons in the sense of Eq. (13). While approximate boson sampling becomes trivial in this case [14], approximate MBCS is at least as complex as when perfectly identical input photons are used.

Since detectors with high temporal resolution (< 1 ns) and single photons with large coherence times (> 1 μ s) are readily available today experimentally [36], the requirement of time-resolved measurements in the implementation of the MBCS problem can be readily fulfilled. Moreover, an implementation of MBCS has the advantage to ease the difficulties faced in the production of identical photons. Indeed, photons of approximately equal colors ($\Delta\omega \gg |\omega_s - \omega_{s'}| \ \forall s \neq s'$) are not needed any more, unlike in the original approximate boson sampling problem. This furthermore paves the way towards the use of photons of arbitrarily small bandwidth $\Delta\omega$, where the indistinguishability in the emission times ($1/\Delta\omega \gg |t_{0s} - t_{0s'}| \ \forall s, s'$) can be easily achieved.

In conclusion, all these results represent an important stepping-stone towards a full fundamental understanding of the complexity of multiphoton interference of photons

of arbitrary spectra in linear optical networks, when the information about detection times and polarizations is not ignored. This may lead to “real world” applications in quantum information processing [52] and in quantum optics overcoming the experimental challenge in the production of identical bosons.

Finally, our results can be extended to bosonic interferometric networks with atoms [12, 13, 63], plasmons [64] or mesoscopic many-body systems [65] and are also relevant to the study of the complexity of multiboson correlation interference for different input states [2, 66, 67] and different correlation measurements [68].

ACKNOWLEDGMENTS

The authors are very grateful to S. Aaronson for useful insights and discussions, as well as to K. Ranade for providing insights on the theory of i.i.d. Gaussian matrices.

V.T. acknowledges the support of the German Space Agency DLR with funds provided by the Federal Ministry of Economics and Technology (BMWi) under grant no. DLR 50 WM 1556.

This work was supported by a grant from the Ministry of Science, Research and the Arts of Baden-Württemberg (Az: 33-7533-30-10/19/2).

The authors contributed equally to this letter.

-
- [1] V. Tamma and S. Laibacher, *Phys. Rev. Lett.* **114**, 243601 (2015).
 - [2] V. Tamma and S. Laibacher, *Phys. Rev. A* **90**, 063836 (2014).
 - [3] V. Tamma and J. Seiler, *New J. Phys.* **18**, 032002 (2016).
 - [4] J.-W. Pan, Z.-B. Chen, C.-Y. Lu, H. Weinfurter, A. Zeilinger, and M. Żukowski, *Rev. Mod. Phys.* **84**, 777 (2012).
 - [5] E. Knill, R. Laflamme, and G. J. Milburn, *Nature* **409**, 46 (2001).
 - [6] R. Hanbury Brown and R. Q. Twiss, *Nature* **178**, 1046 (1956).
 - [7] K. R. Motes, J. P. Olson, E. J. Rabeaux, J. P. Dowling, S. J. Olson, and P. P. Rohde, *Phys. Rev. Lett.* **114**, 170802 (2015).
 - [8] M. D’Angelo, A. Garuccio, and V. Tamma, *Phys. Rev. A* **77**, 063826 (2008).
 - [9] T. B. Pittman, Y. H. Shih, D. V. Strekalov, and A. V. Sergienko, *Phys. Rev. A* **52**, R3429 (1995).
 - [10] C. K. Hong, Z. Y. Ou, and L. Mandel, *Phys. Rev. Lett.* **59**, 2044 (1987).
 - [11] C. O. Alley and Y. H. Shih, in *Proceedings of the Second International Symposium on Foundations of Quantum Mechanics in the Light of New Technology* (Physical Soc. of Japan, Tokyo, 1986) pp. 47–52, editor: Namiki, M; Y. H. Shih and C. O. Alley, *Phys. Rev. Lett.* **61**, 2921 (1988).
 - [12] A. M. Kaufman, B. J. Lester, C. M. Reynolds, M. L. Wall, M. Foss-Feig, K. R. A. Hazzard, A. M. Rey, and C. A. Regal, *Science* **345**, 306 (2014).
 - [13] R. Lopes, A. Imanaliev, A. Aspect, M. Cheneau, D. Boiron, and C. I. Westbrook, *Nature* **520**, 66 (2015).
 - [14] S. Aaronson and A. Arkhipov, in *Proceedings of the forty-third annual ACM symposium on Theory of computing* (ACM, New York, 2011) pp. 333–342.
 - [15] V. Tamma and S. Laibacher, *J. Mod. Opt.* **63**, 41 (2015).
 - [16] X.-C. Yao, T.-X. Wang, P. Xu, H. Lu, G.-S. Pan, X.-H. Bao, C.-Z. Peng, C.-Y. Lu, Y.-A. Chen, and J.-W. Pan, *Nature Photon.* **6**, 225 (2012).
 - [17] Y.-S. Ra, M. C. Tichy, H.-T. Lim, O. Kwon, F. Mintert, A. Buchleitner, and Y.-H. Kim, *Nature Commun.* **4**, 2451 (2013).
 - [18] B. J. Metcalf, N. Thomas-Peter, J. B. Spring, D. Kundys, M. A. Broome, P. C. Humphreys, X.-M. Jin, M. Barbieri, W. S. Kolthammer, J. C. Gates, and others, *Nature Commun.* **4**, 1356 (2013).
 - [19] M. A. Broome, A. Fedrizzi, S. Rahimi-Keshari, J. Dove, S. Aaronson, T. C. Ralph, and A. G. White, *Science* **339**, 794 (2013).
 - [20] A. Crespi, R. Osellame, R. Ramponi, D. J. Brod, E. F. Galvão, N. Spagnolo, C. Vitelli, E. Maiorino, P. Mataloni, and F. Sciarrino, *Nature Photon.* **7**, 545 (2013).
 - [21] M. Tillmann, B. Dakić, R. Heilmann, S. Nolte, A. Szameit, and P. Walther, *Nature Photon.* **7**, 540 (2013).
 - [22] M. Tillmann, S.-H. Tan, S. E. Stoeckl, B. C. Sanders, H. de Guise, R. Heilmann, S. Nolte, A. Szameit, and P. Walther, *Phys. Rev. X* **5**, 041015 (2015).
 - [23] J. B. Spring, B. J. Metcalf, P. C. Humphreys, W. S. Kolthammer, X.-M. Jin, M. Barbieri, A. Datta, N. Thomas-Peter, N. K. Langford, D. Kundys, J. C. Gates,

- B. J. Smith, P. G. R. Smith, and I. A. Walmsley, *Science* **339**, 798 (2013).
- [24] N. Spagnolo, C. Vitelli, M. Bentivegna, D. J. Brod, A. Crespi, F. Flamini, S. Giacomini, G. Milani, R. Ramponi, P. Mataloni, R. Osellame, E. F. Galvao, and F. Sciarrino, *Nature Photon.* **8**, 615 (2014).
- [25] J. Carolan, J. D. A. Meinecke, P. Shadbolt, N. J. Russell, N. Ismail, K. Wörhoff, T. Rudolph, M. G. Thompson, J. L. O’Brien, J. C. F. Matthews, and A. Laing, *Nature Photon.* **8**, 621 (2013).
- [26] M. Bentivegna, N. Spagnolo, C. Vitelli, F. Flamini, N. Viggianiello, L. Latmiral, P. Mataloni, D. J. Brod, E. F. Galvão, A. Crespi, R. Ramponi, R. Osellame, and F. Sciarrino, *Sci. Adv.* **1**, e1400255 (2015).
- [27] J. D. Franson, *Science* **339**, 767 (2013).
- [28] T. Ralph, *Nature Photon.* **7**, 514 (2013).
- [29] M. Keller, B. Lange, K. Hayasaka, W. Lange, and H. Walther, *Nature* **431**, 1075 (2004).
- [30] P. Kolchin, C. Belthangady, S. Du, G. Y. Yin, and S. E. Harris, *Phys. Rev. Lett.* **101**, 103601 (2008).
- [31] C. Polycarpou, K. N. Cassemiro, G. Venturi, A. Zavatta, and M. Bellini, *Phys. Rev. Lett.* **109**, 053602 (2012).
- [32] T. Legero, T. Wilk, M. Hennrich, G. Rempe, and A. Kuhn, *Phys. Rev. Lett.* **93**, 070503 (2004).
- [33] T.-M. Zhao, H. Zhang, J. Yang, Z.-R. Sang, X. Jiang, X.-H. Bao, and J.-W. Pan, *Phys. Rev. Lett.* **112**, 103602 (2014).
- [34] Z.-S. Yuan, Y.-A. Chen, S. Chen, B. Zhao, M. Koch, T. Strassel, Y. Zhao, G.-J. Zhu, J. Schmiedmayer, and J.-W. Pan, *Phys. Rev. Lett.* **98**, 180503 (2007).
- [35] X.-H. Bao, A. Reingruber, P. Dietrich, J. Rui, A. Dück, T. Strassel, L. Li, N.-L. Liu, B. Zhao, and J.-W. Pan, *Nat. Phys.* **8**, 517 (2012).
- [36] M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov, *Rev. Sci. Instrum.* **82**, 071101 (2011).
- [37] P. B. R. Nisbet-Jones, J. Dilley, A. Holleczek, O. Barter, and A. Kuhn, *New J. Phys.* **15**, 053007 (2013).
- [38] D. P. Monroe, *Physics* **5**, 86 (2012).
- [39] V. Tamma, *Int. J. Quantum Inf.* **12**, 1560017 (2014).
- [40] V. Tamma, *Quantum Inf. Process.* (2015), doi:10.1007/s11128-015-1190-y.
- [41] V. Tamma, *Quantum Inf. Process.* (2015), doi:10.1007/s11128-015-1189-4.
- [42] V. Tamma, H. Zhang, X. He, A. Garuccio, W. P. Schleich, and Y. Shih, *Phys. Rev. A* **83**, 020304(R) (2011).
- [43] V. Tamma, H. Zhang, X. He, A. Garuccio, and Y. H. Shih, *J. Mod. Opt.* **56**, 2125 (2009).
- [44] V. Tamma, C. O. Alley, W. P. Schleich, and Y. H. Shih, *Found. Phys.* **42**, 111 (2012).
- [45] C. H. Bennett and S. J. Wiesner, *Phys. Rev. Lett.* **69**, 2881 (1992).
- [46] D. L. Moehring, P. Maunz, S. Olmschenk, K. C. Younge, D. N. Matsukevich, L.-M. Duan, and C. Monroe, *Nature* **449**, 68 (2007).
- [47] Z.-S. Yuan, Y.-A. Chen, B. Zhao, S. Chen, J. Schmiedmayer, and J.-W. Pan, *Nature* **454**, 1098 (2008).
- [48] D. M. Greenberger, M. A. Horne, and A. Zeilinger, in *Bell’s Theorem, Quantum Theory and Conceptions of the Universe*, edited by M. Kafatos (Kluwer Academic Publishers, 1989) pp. 69–72.
- [49] D. Bouwmeester, J.-W. Pan, M. Daniell, H. Weinfurter, and A. Zeilinger, *Phys. Rev. Lett.* **82**, 1345 (1999).
- [50] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, *Phys. Rev. Lett.* **70**, 1895 (1993).
- [51] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, *Phys. Rev. Lett.* **71**, 4287 (1993).
- [52] A. Holleczek, O. Barter, A. Rubenok, J. Dilley, P. B. R. Nisbet-Jones, G. Langfahl-Klabes, G. D. Marshall, C. Sparrow, J. L. O’Brien, K. Poulios, Kuhn, Axel, and Matthews, Jonathan C. F., (2015), arXiv:1508.03266.
- [53] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, *Phys. Rev. Lett.* **73**, 58 (1994).
- [54] R. Loudon, *The quantum theory of light*, 3rd ed., Oxford science publications (Oxford University Press, Oxford ; New York, 2000).
- [55] V. Tamma and S. Laibacher, *Quantum Inf. Process.* **15**, 1241 (2015).
- [56] The case of boson bunching at the detectors can be neglected for $M \gg N$ [14].
- [57] The Supplemental Material can be found at the end of this file and contains the references [69–71].
- [58] For a more mathematical definition of the MBCS problem in the exact and the approximate case, we refer to the Supplemental Material [57].
- [59] R. J. Glauber, *Rev. Mod. Phys.* **78**, 1267 (2006).
- [60] We refer to section III of the Supplemental Material [57] for a more detailed formal proof.
- [61] M. Jerrum, A. Sinclair, and E. Vigoda, *J. ACM* **51**, 671 (2004).
- [62] The case $0 < a(s, s') < 1$, where the number of N -photon interference events is only a finite fraction of the total number of possible events, is beyond the scope of this letter and will be addressed in a future publication.
- [63] C. Shen, Z. Zhang, and L.-M. Duan, *Phys. Rev. Lett.* **112**, 050504 (2014).
- [64] S. Varró, N. Kroó, D. Oszetzky, A. Nagy, and A. Czitrovsky, *J. Mod. Opt.* **58**, 2049 (2011).
- [65] J.-D. Urbina, J. Kuipers, S. Matsumoto, Q. Hummel, and K. Richter, *Phys. Rev. Lett.* **116**, 100401 (2016).
- [66] A. Lund, A. Laing, S. Rahimi-Keshari, T. Rudolph, J. O’Brien, and T. Ralph, *Phys. Rev. Lett.* **113**, 100502 (2014).
- [67] J. P. Olson, K. P. Seshadreesan, K. R. Motes, P. P. Rohde, and J. P. Dowling, *Phys. Rev. A* **91**, 022317 (2015).
- [68] R. J. Glauber, L. A. Orozco, K. Vogel, W. P. Schleich, and H. Walther, *Phys. Scripta* **T140**, 014002 (2010).
- [69] L. Stockmeyer, in *Proceedings of the Fifteenth Annual ACM Symposium on Theory of Computing*, STOC ’83 (ACM, New York, NY, USA, 1983) pp. 118–126.
- [70] S. Toda, *SIAM J. Comput.* **20**, 865 (1991).
- [71] G. Kuperberg, *Theory Comput.* **11**, 183 (2015).

From the Physics to the Computational Complexity of Multiboson Correlation Interference: Supplemental Material

I. THE MULTIBOSON CORRELATION SAMPLING (MBCS) PROBLEM

Here, we formally define the MultiBoson Correlation Sampling (MBCS) problem in linear interferometers described by a unitary $M \times M$ matrix chosen randomly according to the Haar measure.

We first introduce the notion of families of interferometer input states $\{|1[\xi_s]\rangle_s\}_{s \in \mathcal{S}}$, at the input ports $s \in \mathcal{S}$, defined by the sets $\{\xi_s\}_{s \in \mathcal{S}}$ of N complex spectral distributions

$$\xi_s(\omega) := \mathbf{v}_s \xi_s(\omega - \omega_s) e^{i\omega t_{0s}}, \quad (\text{S1})$$

with square integrable spectral shapes $\xi_s(\omega - \omega_s)$ centered around $\omega = \omega_s$, polarizations \mathbf{v}_s , central frequencies ω_s , and emission times t_{0s} :

Definition 1 (Families of input states). Let I be the set of square normalized, complex spectral distributions which fulfill the narrow-bandwidth approximation. For given sets $F_N \subseteq I^N$, with $N \in \mathbb{N}$, of N -tuples $\{\xi_s\}_{s \in \mathcal{S}} \in F_N$ of single-photon spectra, we define the family $F := \{F_N\}_{N \in \mathbb{N}}$. Further, we denote as \mathcal{F} the set of all possible families F .

Secondly, we formally define all the possible samples that can be detected at the interferometer output in the MBCS problem by discretizing the detection-time axis into bins of width $2T_I$ (integration time) much smaller than the temporal widths of the photons and centered at times $t_k := 2T_I k$. Here, $k = k_{\min}, k_{\min} + 1, \dots, k_{\max}$, where $k_{\min}, k_{\max} \in \mathbb{Z}$ define the temporal interval where detections can occur. From now on, we will refer to the time samples $\{t_d\}_{d \in \mathcal{D}}$ only in terms of the N integers $\{k_d = t_d/(2T_I)\}_{d \in \mathcal{D}}$ and define each possible *overall sample* as $\mathfrak{S} := (\mathcal{D}; \{k_d\}, \{\mathbf{p}_d\})$, with $\mathbf{p}_d \in \{\mathbf{e}_1, \mathbf{e}_2\}$ for a fixed orthonormal polarization basis $\{\mathbf{e}_1, \mathbf{e}_2\}$.

The probability distribution

$$\mathcal{P}_F = \mathcal{P}_F(\{\xi_s\} \in F_N, A \in \mathcal{U}_{M,N}) \quad (\text{S2})$$

associated with all the possible samples \mathfrak{S} is defined by a given rectangular $M \times N$ submatrix

$$A := [\mathcal{U}_{d,s}]_{\substack{d=1,\dots,M \\ s \in \mathcal{S}}} \in \mathcal{U}_{M,N}$$

of the interferometer matrix \mathcal{U} , where $\mathcal{U}_{M,N}$ is the set of $M \times N$ matrices with orthogonal columns, and by a given set of complex spectral distributions $\{\xi_s\} \in F_N$ for the N input photons, with $F = \{F_N\}_{N \in \mathbb{N}} \in \mathcal{F}$.

As shown in the main letter, defining the matrices

$$\mathcal{T}_{\{k_d, \mathbf{p}_d\}}^{(\mathcal{D}, \mathcal{S})} = \mathcal{T}_{\{t_{k_d}, \mathbf{p}_d\}}^{(\mathcal{D}, \mathcal{S})} := \left[\mathcal{U}_{d,s}(\mathbf{p}_d \cdot \chi_s(2T_I k_d)) \right]_{\substack{d \in \mathcal{D} \\ s \in \mathcal{S}}} \quad (\text{S3})$$

where

$$\chi_s(t) = \mathbf{v}_s \chi_s(t - t_{0s} - \Delta t) e^{i\omega_s(t - t_{0s} - \Delta t)} \quad (\text{S4})$$

are the Fourier transforms of the spectra $\xi_s(\omega)$ in Eq. (S1) (Δt is the delay the photons pick up in the interferometer), the probability $p_{\mathfrak{S}}$ associated with the sample \mathfrak{S} , when sampling from the distribution \mathcal{P}_F in Eq. (S2), is

$$p_{\mathfrak{S}} := \Pr_{\mathcal{P}_F}[\mathfrak{S}] = P_{\{t_{k_d}, \mathbf{p}_d\}}^{(\mathcal{D}, \mathcal{S})} = (2T_I)^N \left| \text{perm } \mathcal{T}_{\{k_d, \mathbf{p}_d\}}^{(\mathcal{D}, \mathcal{S})} \right|^2. \quad (\text{S5})$$

For samples \mathfrak{S}_{id} with identical detection times $k_d = k \ \forall d \in \mathcal{D}$ and polarizations $\mathbf{p}_d = \mathbf{p} \ \forall d \in \mathcal{D}$, this simplifies to

$$p_{\mathfrak{S}_{\text{id}}} = (2T_I)^N \prod_{s \in \mathcal{S}} |\mathbf{p} \cdot \chi_s(2T_I k)|^2 \left| \text{perm } \mathcal{U}^{(\mathcal{D}, \mathcal{S})} \right|^2. \quad (\text{S6})$$

Following Aaronson and Arkhipov in [S1], it is reasonable to represent the elements of the interferometer matrix as rational numbers $(x+iy)/2^{\text{poly}(N)}$ with integers x and y . Analogously, the same holds for the values T_I , $\chi_s(t_d - t_{0s} - \Delta t)$, $\mathbf{p}_d \cdot \mathbf{v}_s$, and $\exp(i\omega_s(t_d - t_{0s} - \Delta t))$, with $s \in \mathcal{S}$ (notice that this representation is reasonable since all these given complex values describing an MBCS experiment can be approximated with high enough precision by choosing $\text{poly}(N)$ sufficiently large).

We emphasize that, while we will prove the hardness of the MBCS problem assuming the rational representation of these numbers, this proof can easily be generalized to a representation in terms of algebraic numbers which are dense in \mathbb{C} (more information can be found in App. B).

Theorem 1 (Exponential size of the probabilities). *Assume that the interferometer matrix and the temporal distributions are given in a rational representation, as described above. Then, independently of the specific choice of $A \in \mathfrak{U}_{M,N}$, $F = \{F_N\} \in \mathcal{F}$, and $\{\xi_s\}_{s \in \mathcal{S}} \in F_N$, all the probabilities (S5) in the probability distribution \mathcal{P}_F are at most exponentially small,*

$$p_{\mathfrak{S}} \geq 2^{-\text{poly}(N)} \quad \forall \mathfrak{S}.$$

Alternatively, the same result holds if we instead assume that the values are represented by algebraic numbers (which are dense in \mathbb{C}).

Proof. This is demonstrated in App. A. ■

Furthermore, the probabilities can be represented as (see App. A)

$$p_{\mathfrak{S}} = \frac{w_{\mathfrak{S}}}{2^{\text{poly}(N)}}$$

with an integer $w_{\mathfrak{S}}$, which ensures that an MBCS oracle as it will be defined in Definition 2 (using a random input string r of length at most polynomial in N) is able to sample from a probability distribution equal or arbitrarily close to the exact probability distribution in Eq. (S2) where the probability for each sample \mathfrak{S} is defined by Eq. (S5).

We can finally define an MBCS oracle as:

Definition 2 (Definition of an MBCS oracle in analogy to [S1]). Let \mathcal{O}_F be an oracle that takes as input an $M \times N$ matrix $A \in \mathfrak{U}_{M,N}$, an N -tuple $\{\xi_s\}_{s \in \mathcal{S}} \in F_N$ from a given family $F \in \mathcal{F}$, an error bound $\beta > 0$ (encoded in unary as $0^{1/\beta}$ to ensure a scaling of resources with $1/\beta$), and a string $r \in \{0,1\}^{\text{poly}(N)}$ which is its only source of randomness. Let $\mathcal{P}_{\mathcal{O}_F} = \mathcal{P}_{\mathcal{O}_F}(\{\xi_s\}, A; \beta)$ be the distribution over the outputs of \mathcal{O}_F if A , $\{\xi_s\}$, and β are fixed but r is uniformly random. Then, \mathcal{O}_F is called an *exact MBCS oracle for the family F* if $\mathcal{P}_{\mathcal{O}_F}(\{\xi_s\}, A; \beta) \equiv \mathcal{P}_F(\{\xi_s\}, A)$ for all $N \in \mathbb{N}$, $A \in \mathfrak{U}_{M,N}$, $\{\xi_s\} \in F_N$, and $\beta > 0$. Further, \mathcal{O}_F is an *approximate MBCS oracle for the family F* if $\|\mathcal{P}_{\mathcal{O}_F}(\{\xi_s\}, A; \beta) - \mathcal{P}_F(\{\xi_s\}, A)\| \leq \beta$ for all $N \in \mathbb{N}$, $A \in \mathfrak{U}_{M,N}$, $\{\xi_s\} \in F_N$, and $\beta > 0$, where $\|\mathcal{P}_{\mathcal{O}_F}(\{\xi_s\}, A; \beta) - \mathcal{P}_F(\{\xi_s\}, A)\| := 1/2 \sum_{\mathfrak{S}} |\Pr_{\mathcal{P}_{\mathcal{O}_F}}[\mathfrak{S}] - \Pr_{\mathcal{P}_F}[\mathfrak{S}]|$.

II. THE COMPLEXITY OF THE EXACT MBCS PROBLEM

Here, we formally demonstrate the complexity of the exact MBCS problem for the set \mathcal{E} of families E defined as:

Definition 3 (Set \mathcal{E} of “complex” families in the exact MBCS problem). We define $\mathcal{E} \subseteq \mathcal{F}$ (with \mathcal{F} defined in Definition 1) as the subset of families $E := \{E_N\}_{N \in \mathbb{N}}$ which fulfill the condition

$$\forall N \in \mathbb{N}, \forall \{\xi_s\} \in E_N : \quad 0 < a(s, s') \leq 1 \quad \forall s, s' \in \mathcal{S}, \quad (\text{S7})$$

with $a(s, s') := |\mathbf{v}_s \cdot \mathbf{v}_{s'}| \int_{-\infty}^{\infty} dt |\chi_s(t - t_{0s})| |\chi_{s'}(t - t_{0s'})|$.

We first introduce the following theorem:

Theorem 2. *Let $E = \{E_N\}_{N \in \mathbb{N}} \in \mathcal{E}$. It is then ensured that a sequence $\{(k_N, \mathbf{p}_N)\}_{N \in \mathbb{N}}$ of time-polarization tuples, with $k_N \in \{k_{\min}, \dots, k_{\max}\}$ and $\mathbf{p}_N \in \{\mathbf{e}_1, \mathbf{e}_2\}$, exists such that*

$$|\mathbf{p}_N \cdot \chi_s(2T_I k_N)|^2 > 0 \quad \forall s \in \mathcal{S}.$$

For any given N , the tuple (k_N, \mathbf{p}_N) can be found in polynomial time.

Proof of Theorem 2. As already discussed in the main letter, the condition (S7) for a fixed N directly implies the existence of at least one time bin k_N and one polarization \mathbf{p}_N for which all N amplitudes $\mathbf{p}_N \cdot \chi_s(2T_I k_N)$, with $s \in \mathcal{S}$, are non-vanishing.

Moreover, due to the finite number $L := k_{\max} - k_{\min} + 1$ of time bins in the interval $[k_{\min}, k_{\max}]$, (k_N, \mathbf{p}_N) can be found in polynomial time. ■

We can now formulate the main theorem on the complexity of exact MBCS:

Theorem 3 (Main theorem on the complexity of exact MBCS). *If \mathcal{O}_E is an exact MBCS oracle for a given family $E \in \mathcal{E}$, then $\text{P}^{\#P} \subseteq \text{BPP}^{\text{NP}^{\mathcal{O}_E}}$. This implies that the polynomial hierarchy collapses to the third level if the exact MBCS problem for states in the family E can be solved in polynomial time by a classical computer.*

Proof of Theorem 3. If a matrix $X \in \mathbb{R}^{N \times N}$ and a parameter $g \in [1 + 1/\text{poly}(N), \text{poly}(N)]$ are given, it is #P-hard to approximate $|\text{perm } X|^2$ to within a multiplicative factor g [S1].

We now show that, given an MBCS oracle \mathcal{O}_E for a family $E \in \mathcal{E}$ (with \mathcal{E} defined in Definition 3), it is possible to perform this approximation in $\text{FBPP}^{\text{NP}^{\mathcal{O}_E}}$.

As shown in [S1], given $\gamma := 1/\|X\| \geq 2^{-\text{poly}(N)}$, it is possible for any $M \geq 2N$ to find in polynomial time a unitary $M \times M$ matrix \mathcal{U} which contains γX as its top-left $N \times N$ submatrix, i.e.

$$\gamma X = [\mathcal{U}_{d,s}]_{\substack{d=1,\dots,N \\ s=1,\dots,N}}.$$

Given $\mathcal{S} := \{1, 2, \dots, N\}$, the matrix $A = [\mathcal{U}_{d,s}]_{\substack{d=1,\dots,M \\ s \in \mathcal{S}}} \in \mathfrak{U}_{M,N}$ and the spectra $\{\xi_s\}_{s \in \mathcal{S}} \in E_N$ induce the probability distribution $\mathcal{P}_E = \mathcal{P}_E(\{\xi_s\}, A)$. From Theorem 2, a tuple (k_N, \mathbf{p}_N) exists such that $\prod_{s \in \mathcal{S}} |\mathbf{p}_N \cdot \chi_s(2T_I k_N)|^2 > 0$. For the sample

$$\mathfrak{S}^* := (\mathcal{D}^*; \underbrace{\{k_N, \dots, k_N\}}_{N \text{ times}}, \underbrace{\{\mathbf{p}_N, \dots, \mathbf{p}_N\}}_{N \text{ times}}),$$

with

$$\mathcal{D}^* := \{1, 2, \dots, N\},$$

the probability in Eq. (S6) becomes

$$p_{\mathfrak{S}^*} = \Pr_{\mathcal{P}_E}[\mathfrak{S}^*] = \gamma^{2N} (2T_I)^N \prod_{s \in \mathcal{S}} |\mathbf{p}_N \cdot \chi_s(t_N)|^2 |\text{perm } X|^2. \quad (\text{S8})$$

According to Definition 2, the exact MBCS oracle \mathcal{O}_E samples from the probability distribution $\mathcal{P}_{\mathcal{O}_E}(\{\xi_s\}, A; \beta) \equiv \mathcal{P}_E(\{\xi_s\}, A)$ returning the value $\mathcal{O}_E(\{\xi_s\}, A, r) = \mathfrak{S}^*$ with probability

$$p_{\mathfrak{S}^*} = \Pr_{r \in \{0,1\}^{\text{poly}(N)}}[\mathcal{O}_E(\{\xi_s\}, A, r) = \mathfrak{S}^*].$$

Defining the Boolean function

$$f : \{0, 1\}^{\text{poly}(N)} \rightarrow \{0, 1\}, r \mapsto \begin{cases} 1 & \mathcal{O}_E(\{\xi_s\}, A, r) = \mathfrak{S}^* \\ 0 & \mathcal{O}_E(\{\xi_s\}, A, r) \neq \mathfrak{S}^* \end{cases}, \quad (\text{S9})$$

we can also express this probability as

$$p_{\mathfrak{S}^*} = \frac{1}{2^{\text{poly}(N)}} \sum_{r \in \{0,1\}^{\text{poly}(N)}} f(r). \quad (\text{S10})$$

Therefore, we can use Stockmeyer's algorithm [S2] to approximate $p_{\mathfrak{S}^*}$ to within a multiplicative factor $g \in [1 + 1/\text{poly}(N), \text{poly}(N)]$ in $\text{FBPP}^{\text{NP}^{\mathcal{O}_E}}$ in time polynomial in N . Consequently, from Eq. (S8), we can approximate $|\text{perm } X|^2$ in $\text{FBPP}^{\text{NP}^{\mathcal{O}_E}}$ as well. Since performing such an approximation is a #P-hard problem [S1], $\text{P}^{\#P} \subseteq \text{BPP}^{\text{NP}^{\mathcal{O}_E}}$. If the MBCS problem could be solved in polynomial time by a classical computer this would imply $\text{P}^{\#P} \subseteq \text{BPP}^{\text{NP}}$, which, by Toda's theorem [S3], would lead to a collapse of the polynomial hierarchy to the third level. ■

III. THE APPROXIMATE MBCS PROBLEM

We consider, for simplicity, a multiboson correlation experiment with polarization-insensitive detectors and states from a family $R := \{R_N\}_{N \in \mathbb{N}} \in \mathcal{F}$ (with \mathcal{F} defined in Definition 1) of input states $\{|1[\xi_s]\rangle_{s \in \mathcal{S}}\}$ defined by input spectra

$$\{\xi_s(\omega)\}_{s \in \mathcal{S}} = \left\{ \mathbf{v} \frac{1}{\sqrt{\pi \Delta \omega}} \text{sinc} \left(\frac{\omega - \omega_s}{\Delta \omega} \right) e^{i\omega t_0} \right\}_{s \in \mathcal{S}}$$

with equal emission times $t_{0s} = t_0$, equal polarizations $\mathbf{v}_s = \mathbf{v}$, and equal bandwidths $\Delta\omega_s = \Delta\omega$ but different colors ω_s . For these spectra, the elements of the N -photon interference matrix $a(s, s') := |\mathbf{v}_s \cdot \mathbf{v}_{s'}| \int_{-\infty}^{\infty} dt |\chi_s(t - t_{0s})| |\chi_{s'}(t - t_{0s'})|$ fulfill the condition

$$a(s, s') \simeq 1 \quad \forall s, s'$$

of full temporal overlap. As in section II, we discretize the detection-time axis into time bins of width $2T_I$. Here, as described in the main letter, in each output port a detection can only occur in the time bins $t_k := 2T_I k \in T := [t_0 + \Delta t - 1/\Delta\omega, t_0 + \Delta t + 1/\Delta\omega]$, with $k \in \{k_{\min}, k_{\min} + 1, \dots, k_{\max}\}$, where $k_{\min} := (t_0 + \Delta t - 1/\Delta\omega + T_I)/(2T_I)$ and $k_{\max} := (t_0 + \Delta t + 1/\Delta\omega - T_I)/(2T_I)$. Therefore, the total number of time bins in which a detection is possible is $L := 1/(T_I \Delta\omega)$. Given the output probability distribution

$$\mathcal{P}_R := \mathcal{P}_R(\{\xi_s\}_{s \in \mathcal{S}} \in R_N, A \in \mathfrak{U}_{M,N}),$$

for a given sample $\mathfrak{S} := (\mathcal{D}; \{k_d\})$, the probability

$$p_{\mathfrak{S}} := \Pr_{\mathcal{P}_R}[\mathfrak{S}] = P_{\{t_{k_d}\}}^{(\mathcal{D}, \mathcal{S})} = (T_I \Delta\omega)^N \left| \text{perm} \left([\mathcal{U}_{d,s}^{(\mathcal{D}, \mathcal{S})} e^{i\omega_s t_{k_d}}]_{d \in \mathcal{D}, s \in \mathcal{S}} \right) \right|^2,$$

derived in the main letter, takes the form

$$p_{\mathfrak{S}} = \frac{1}{L^N} \left| \text{perm} \left([\mathcal{U}_{d,s}^{(\mathcal{D}, \mathcal{S})} e^{2iT_I \omega_s k_d}]_{d \in \mathcal{D}, s \in \mathcal{S}} \right) \right|^2. \quad (\text{S11})$$

We can now formulate the following theorem on the computational power of an approximate MBCS oracle for the family R :

Theorem 4 (Computational power of an approximate MBCS oracle for the family R of input states). *Let \mathcal{O}_R be an approximate oracle for the MBCS problem for the family R and $\varepsilon, \delta > 0$ given error bounds. It is then possible to approximate the modulus square of the permanent of a random Gaussian $N \times N$ matrix to within an additive error $\pm \varepsilon N!$ and with success probability larger than $1 - \delta$ in $\text{FBPP}^{\text{NP}^{\mathcal{O}_R}}$ in time polynomial in N , $1/\varepsilon$, and $1/\delta$.*

Proof of Theorem 4. Let X be a complex $N \times N$ matrix whose entries are randomly picked according to a standard complex normal probability distribution $\mathcal{N}(0, 1)_{\mathbb{C}}$. We will adapt the arguments found in [S1] to give an algorithm in $\text{FBPP}^{\text{NP}^{\mathcal{O}_R}}$ that performs the required approximation in polynomial time. The main idea is to introduce an $M \times N$ matrix $A = [\mathcal{U}_{d,s}]_{d=1, \dots, M, s \in \mathcal{S}} \in \mathfrak{U}_{M,N}$ (as in the exact case, A is a rectangular submatrix of a Haar-random unitary interferometer matrix \mathcal{U} corresponding to the input configuration $\mathcal{S} := \{1, 2, \dots, N\}$) such that a specific sample $\mathfrak{S}^* := (\mathcal{D}^*, \{k_d^*\})$ occurs with probability $p_{\mathfrak{S}^*} \propto |\text{perm } X|^2$, which can be estimated using the approximate MBCS oracle defined in Definition 2.

1. In order to rule out the possibility that the oracle can willingly sabotage the output probability of the sample \mathfrak{S}^* in which we are interested, \mathfrak{S}^* has to be picked randomly. Therefore, the time sample $\{k_d^*\}$ is generated by randomly picking N time bins $t_{k_d^*} = 2T_I k_d^* \in T$ according to a uniform probability distribution. Given the structure of the probabilities in Eq. (S11), it is useful to define a matrix \tilde{X} which incorporates the inverse of the phase factors corresponding to the randomly chosen time sample $\{k_d^*\}$, i.e.

$$\tilde{X}_{i,j} := X_{i,j} e^{-2iT_I \omega_{s_j} k_{d_i}^*},$$

where d_i and s_i are the i -th elements of \mathcal{D} and \mathcal{S} , respectively. Since the elements of X are i.i.d. Gaussian random variables, the same holds for the elements of \tilde{X} , as shown in App. C.

2. An $M \times N$ matrix $A \in \mathfrak{U}_{M,N}$ is generated with the following properties: A is distributed like the submatrix $[\mathcal{U}_{d,s}]_{d=1, \dots, M, s \in \mathcal{S}}$ of a Haar-distributed $M \times M$ unitary matrix \mathcal{U} and it contains $\tilde{X}' := \tilde{X}/\sqrt{M}$ as a uniformly random submatrix. As shown in [S1], since \tilde{X} is a Gaussian matrix this is possible to achieve in BPP^{NP} with a failure probability

$$\Pr[\text{hiding failed}] \leq \frac{\delta}{4}, \quad (\text{S12})$$

provided

$$M = K \frac{N^5}{\delta} \log^2 \frac{N}{\delta} \quad (\text{S13})$$

with a sufficiently large constant K . The random output-port sample that corresponds to the position of $\tilde{X}' = [\mathcal{U}_{d,s}]_{\substack{d \in \mathcal{D}^* \\ s \in \mathcal{S}}}$ inside of A is denoted as \mathcal{D}^* . Thus, for the random sample $\mathfrak{S}^* := (\mathcal{D}^*; \{k_d^*\})$, Eq. (S11) becomes

$$p_{\mathfrak{S}^*} = \frac{1}{L^N} \left| \text{perm} \left([M^{-1/2} \tilde{X}_{i,j} e^{2iT_I \omega_{s_j} k_{d_i}^*}]_{\substack{i=1,\dots,N \\ j=1,\dots,N}} \right) \right|^2 = \frac{1}{L^N M^N} |\text{perm } X|^2. \quad (\text{S14})$$

3. While $p_{\mathfrak{S}^*}$ describes the probability for the sample \mathfrak{S}^* within the exact probability distribution $\mathcal{P}_R = \mathcal{P}_R(\{\xi_s\}, A)$, we define

$$q_{\mathfrak{S}^*} := \Pr_{\mathcal{P}_{\mathcal{O}_R}} [\mathfrak{S}^*] = \Pr_{r \in \{0,1\}^{\text{poly}(N)}} [\mathcal{O}_R(\{\xi_s\}, A, r; \beta) = \mathfrak{S}^*]$$

as the probability for the sample \mathfrak{S}^* within the probability distribution $\mathcal{P}_{\mathcal{O}_R} = \mathcal{P}_{\mathcal{O}_R}(\{\xi_s\}, A; \beta)$ of the approximate MBCS oracle \mathcal{O}_R (as shown in App. A, all probabilities $p_{\mathfrak{S}}$ are at most exponentially small and it is thus ensured that an oracle \mathcal{O}_R as defined in Definition 2 can sample according to a probability distribution $\mathcal{P}_{\mathcal{O}_R}(\{\xi_s\}, A; \beta)$ arbitrarily close to $\mathcal{P}_R(\{\xi_s\}, A)$).

In analogy to Eqs. (S9) and (S10), we can also define a Boolean function

$$f : \{0,1\}^{\text{poly}(N)} \rightarrow \{0,1\}, r \mapsto \begin{cases} 1 & \mathcal{O}_R(\{\xi_s\}, A, r; \beta) = \mathfrak{S}^* \\ 0 & \mathcal{O}_R(\{\xi_s\}, A, r; \beta) \neq \mathfrak{S}^* \end{cases},$$

and write

$$q_{\mathfrak{S}^*} = \frac{1}{2^{\text{poly}(N)}} \sum_{r \in \{0,1\}^{\text{poly}(N)}} f(r).$$

This makes it evident that Stockmeyer's algorithm [S2] can be used to find a value $\tilde{q}_{\mathfrak{S}^*}$ in $\text{FBPP}^{\text{NP}^{\mathcal{O}_R}}$ that approximates $q_{\mathfrak{S}^*}$ to within a multiplicative factor $(1 + \alpha) \in [1 + 1/\text{poly}(N), \text{poly}(N)]$, such that

$$\Pr [q_{\mathfrak{S}^*}/(1 + \alpha) \leq \tilde{q}_{\mathfrak{S}^*} \leq (1 + \alpha)q_{\mathfrak{S}^*}] \geq 1 - \frac{1}{2^M} \quad (\text{S15})$$

in time polynomial in M and $1/\alpha$ [S2].

4. By using Definition 2 of the approximate MBCS oracle and Eq. (S15) for $\alpha = \varepsilon\delta/16$, we show in App. D that the estimate $L^N M^N \tilde{q}_{\mathfrak{S}^*}$ of the squared permanent of X satisfies the condition

$$\Pr \left[\left| |\text{perm } X|^2 - L^N M^N \tilde{q}_{\mathfrak{S}^*} \right| > \varepsilon N! \right] < \frac{\delta}{2} + \frac{1}{2^M}. \quad (\text{S16})$$

Adding to Eq. (S16) the probability of failure for the hiding of \tilde{X}' from Eq. (S12) and recalling Eq. (S13) which ensures $2^{-M} < \delta/4$, we find that the total probability of failure is smaller than δ , as required.

Further, the algorithm runs in a time polynomial in N , $1/\delta$, and $1/\varepsilon$ since the hiding procedure in step 2 is polynomial in time with respect to N and $1/\delta$ and the running time of Stockmeyer's algorithm (used in step 3) is polynomial in N and $1/\alpha$, where $\alpha = \varepsilon\delta/16$ was chosen. ■

In [S1], the authors argue that approximating the modulus square of the permanent of a Gaussian matrix is a #P-hard problem if two reasonable conjectures are true. Under this assumption, the following theorem holds:

Theorem 5. *Let \mathcal{O}_R be an approximate MBCS oracle for the family R . If the approximate MBCS problem for R can be solved in polynomial time by a classical computer, the polynomial hierarchy collapses to the third level.*

Proof of Theorem 5. Theorem 4 states that it is possible to approximate the modulus square of a permanent in $\text{FBPP}^{\text{NP}^{\mathcal{O}_R}}$, given an oracle \mathcal{O}_R for the family R . If this approximation is indeed #P-hard, as argued in [S1], it follows that $\text{P}^{\#P} \subseteq \text{BPP}^{\text{NP}^{\mathcal{O}_R}}$. Further, if the MBCS problem for states of this family can be solved in polynomial time by a classical computer, then $\text{P}^{\#P} \subseteq \text{BPP}^{\text{NP}}$ which implies, by Toda's theorem [S3], that the polynomial hierarchy collapses to the third level. ■

Appendix A: Exponential lower bound on the MBCS probabilities

Here, we show that the assumption of a rational representation $(x + iy)/2^{\text{poly}(N)}$ (with integers x, y) of the elements of the interferometer matrix and of the values of the temporal distributions for all possible time bins results in an exponential lower bound on the non-vanishing detection probabilities $p_{\mathfrak{S}}$.

Using the expression (S5), the definitions of a matrix permanent and of the matrix $\mathcal{T}_{\{k_d, \mathbf{p}_d\}}^{(\mathcal{D}, \mathcal{S})}$ in Eq. (S3), and the explicit expression Eq. (S4) for the functions $\chi_s(t)$, we find

$$p_{\mathfrak{S}} = (2T_I)^N \sum_{\sigma, \sigma'} \left[\prod_{d \in \mathcal{D}} \mathcal{U}_{d, \sigma'(d)}^* \mathcal{U}_{d, \sigma(d)} (\mathbf{p}_d \cdot \mathbf{v}_{\sigma'(d)})^* (\mathbf{p}_d \cdot \mathbf{v}_{\sigma(d)}) \right. \\ \times \prod_{d \in \mathcal{D}} (\chi_{\sigma'(d)}(t_d - t_{0\sigma'(d)} - \Delta t))^* \chi_{\sigma(d)}(t_d - t_{0\sigma(d)} - \Delta t) \\ \left. \times \prod_{d \in \mathcal{D}} e^{-i\omega_{\sigma'(d)}(t_d - t_{0\sigma'(d)} - \Delta t)} e^{i\omega_{\sigma(d)}(t_d - t_{0\sigma(d)} - \Delta t)} \right]$$

Since all $8N + 1$ numbers T_I , $\mathcal{U}_{d,s}$ and c.c., $(\mathbf{p}_d \cdot \mathbf{v}_s)$ and c.c., $\chi_s(t_d - t_{0s} - \Delta t)$ and c.c., $\exp[i\omega_s(t_d - t_{0s} - \Delta t)]$ and c.c. are represented as $(x + iy)/2^{\text{poly}(N)}$ (x, y integers), it is immediately clear that the probability has the form

$$p_{\mathfrak{S}} = \frac{1}{2^{\text{poly}(N)}} w_{\mathfrak{S}},$$

with a non-negative integer $w_{\mathfrak{S}}$ and is therefore at most exponentially small. This guarantees that Stockmeyer's algorithm can be used to approximate these probabilities.

The probabilities are also at most exponentially small if these values are represented by algebraic numbers. Indeed, it was shown in [S5] that

$$p_{\mathfrak{S}} \geq 2^{-r(N)}, \quad (\text{SA1})$$

with a polynomial $r(N)$.

Appendix B: Using algebraic numbers instead of rational numbers with polynomial precision

Here, we will show that, instead of assuming that the values $\mathcal{U}_{d,s}$, T_I , $\chi_s(t_d - t_{0s} - \Delta t)$, and $\exp[i\omega_s(t_d - t_{0s} - \Delta t)]$ are represented as rational numbers $(x + iy)/2^{\text{poly}(N)}$ as in [S1], the hardness of MBCS sampling can also be proven if these values are represented by algebraic numbers [S4]. This is appealing because it is possible to find an arbitrarily close algebraic approximation of any complex number since the algebraic numbers are dense in \mathbb{C} .

We emphasize that, in general, an MBCS oracle as defined in Definition 2 now cannot sample from the exact probability distribution \mathcal{P}_F in Eq. (S2) any more. However, as we will demonstrate in the following, the hardness proof in section II is still valid if we define an “exact” MBCS oracle as an oracle which samples from a probability distribution \mathcal{P}_{O_F} with

$$\|\mathcal{P}_{O_F}(\{\xi_s\}, A) - \mathcal{P}_F(\{\xi_s\}, A)\| \leq 2^{-s(N)}, \quad (\text{SB1})$$

where the polynomial $s(N)$ is assumed to dominate the polynomial $r(N)$ from Eq. (SA1) ($s(N) - r(N)$ grows monotonically, and $s(1) > r(1) + 2$). Such an approximation of the exact probability distribution can however still be achieved by an oracle as defined in Definition 2.

Defining the probabilities $q_{\mathfrak{S}} := \Pr_{\mathcal{P}_{O_F}}[\mathfrak{S}]$, Eq. (SB1) implies that

$$|p_{\mathfrak{S}} - q_{\mathfrak{S}}| \leq 2 \cdot 2^{-s(N)} \\ \Leftrightarrow p_{\mathfrak{S}} - 2 \cdot 2^{-s(N)} \leq q_{\mathfrak{S}} \leq p_{\mathfrak{S}} + 2 \cdot 2^{-s(N)} \\ \Rightarrow p_{\mathfrak{S}} \left(1 - 2 \frac{2^{-s(N)}}{p_{\mathfrak{S}}}\right) \leq q_{\mathfrak{S}} \leq p_{\mathfrak{S}} \left(1 + 2 \frac{2^{-s(N)}}{p_{\mathfrak{S}}}\right),$$

which with Ineq. (SA1) becomes

$$\begin{aligned} p_{\mathfrak{S}} \left(1 - 2 \frac{2^{-s(N)}}{2^{-r(N)}} \right) &\leq q_{\mathfrak{S}} \leq p_{\mathfrak{S}} \left(1 + 2 \frac{2^{-s(N)}}{2^{-r(N)}} \right) \\ \Rightarrow p_{\mathfrak{S}} \left(1 - 2^{-(s(N)-r(N)-1)} \right) &\leq q_{\mathfrak{S}} \leq p_{\mathfrak{S}} \left(1 + 2^{-(s(N)-r(N)-1)} \right). \end{aligned}$$

Using the inequality $1 - x \geq 1/(1 + 2x)$ for $0 < x < 1/2$, we find that

$$p_{\mathfrak{S}} \frac{1}{1 + 2^{-(s(N)-r(N)-2)}} \leq q_{\mathfrak{S}} \leq p_{\mathfrak{S}} \left(1 + 2^{-(s(N)-r(N)-2)} \right), \quad (\text{SB2})$$

i.e. that $q_{\mathfrak{S}}$ is multiplicatively close to $p_{\mathfrak{S}}$ to within a factor $1 + 2^{-\text{poly}(N)}$.

The approximation of $p_{\mathfrak{S}}$ to within a multiplicative factor $g \in [1 + \frac{1}{\text{poly}(N)}, \text{poly}(N)]$ can therefore be achieved by approximating $q_{\mathfrak{S}}$ to within a factor $g' := g/(1 + 2^{-(s(N)-r(N)-2)})$. Since $g - 1$ is at most polynomially small, $g' \in [1 + \frac{1}{\text{poly}(N)}, \text{poly}(N)]$ as well. Therefore, Stockmeyer's algorithm tells us that a value $\tilde{q}_{\mathfrak{S}}$ can be found in BPP^{NP} , such that

$$\frac{q_{\mathfrak{S}}}{g'} \leq \tilde{q}_{\mathfrak{S}} \leq g' q_{\mathfrak{S}}.$$

Then, Ineq. (SB2) implies that

$$\frac{p_{\mathfrak{S}}}{g} = \frac{p_{\mathfrak{S}}}{g'(1 + 2^{-(s(N)-r(N)-2)})} \leq \tilde{q}_{\mathfrak{S}} \leq p_{\mathfrak{S}} g' (1 + 2^{-(s(N)-r(N)-2)}) = p_{\mathfrak{S}} g.$$

and the arguments in the hardness proof for the exact MBS in section II still hold if we define “exact” in the sense of Ineq. (SB1).

Further, the proof for the hardness of the approximate MBS problem from section III is still completely valid in the algebraic number representation since an approximate MBS oracle as defined in Definition 2 is still able to sample from a probability distribution that is polynomially close in variation distance to the exact probability distribution.

Appendix C: The distribution of the elements of \tilde{X}

We will now show that, under the assumption that the elements $X_{i,j}$, $i, j = 1, \dots, N$, of a complex $N \times N$ matrix X are i.i.d. random variables with a complex standard normal distribution, the same holds for the elements of \tilde{X} which are defined as

$$\tilde{X}_{i,j} = X_{i,j} e^{i\varphi_{i,j}}.$$

If the elements of X are i.i.d. $\mathcal{N}(0, 1)_{\mathbb{C}}$ variables, their joint probability distribution is

$$f_X(\{X_{i,j}\}) = \prod_{i,j=1}^N \frac{1}{\pi} e^{-|X_{i,j}|^2}.$$

Noting that the Jacobi determinant for the change of variables between the $\{X_{i,j}\}$ and the $\{\tilde{X}_{i,j}\}$ is $\det \mathbf{J} = 1$, we find that the common probability distribution for the elements of \tilde{X} is

$$f_{\tilde{X}}(\{\tilde{X}_{i,j}\}) = f_X(\{\tilde{X}_{i,j} e^{-i\varphi_{i,j}}\}) \cdot \underbrace{\det \mathbf{J}}_{=1} = \prod_{i,j=1}^N \frac{1}{\pi} e^{-|\tilde{X}_{i,j}|^2},$$

where we used that the complex Gaussian distributions are independent of the complex phase.

Therefore, the elements of the matrix \tilde{X} are still i.i.d. $\mathcal{N}(0, 1)_{\mathbb{C}}$ random variables if the elements of X were.

Appendix D: Bound on failure probability of approximation

As in [S1], we define $\Phi_{M,N}$ as the set of all port samples \mathcal{D} and $G_{M,N}$ as the set of bunching-free port samples, i.e. as the set of port samples \mathcal{D} which consist only of pairwise different output port indices. Further, let $\Omega_{L,N}$ be the set of all time samples $\{k_d\}$.

We will now proceed to derive three inequalities which combined yield Ineq. (S16).

1. With $\Delta_{\mathfrak{S}} := |p_{\mathfrak{S}} - q_{\mathfrak{S}}|$, we find the expectation value

$$\begin{aligned} \mathbb{E}_{\mathfrak{S} \in G_{M,N} \otimes \Omega_{L,N}}[\Delta_{\mathfrak{S}}] &:= \frac{\sum_{\mathfrak{S} \in G_{M,N} \otimes \Omega_{L,N}} \Delta_{\mathfrak{S}}}{|G_{M,N}| |\Omega_{L,N}|} \leq \frac{\sum_{\mathfrak{S} \in \Phi_{M,N} \otimes \Omega_{L,N}} \Delta_{\mathfrak{S}}}{|G_{M,N}| |\Omega_{L,N}|} \\ &\stackrel{\text{def}}{=} \frac{2\|\mathcal{P}_{\mathcal{O}_R} - \mathcal{P}_R\|}{|G_{M,N}| |\Omega_{L,N}|} = \frac{2\|\mathcal{P}_{\mathcal{O}_R} - \mathcal{P}_R\|}{\binom{M}{N} L^N} \leq \frac{2\beta}{\binom{M}{N} L^N} < 3\beta \frac{N!}{(LM)^N}, \end{aligned}$$

where, in the penultimate step, we used the Definition 2 of an approximate MBCS oracle and, in the last step, the fact that $M = \omega(N^2)$ (M asymptotically grows faster than N^2) [S1]. Therefore, Markov's inequality gives

$$\Pr_{\mathfrak{S} \in G_{M,N} \otimes \Omega_{L,N}} \left[\Delta_{\mathfrak{S}} > 3\beta \frac{N!}{(LM)^N} \frac{4}{\delta} \right] < \frac{\delta}{4}$$

which, by choosing $\beta = \varepsilon\delta/24$, simplifies to

$$\Pr_{\mathfrak{S} \in G_{M,N} \otimes \Omega_{L,N}} \left[\Delta_{\mathfrak{S}} > \frac{\varepsilon}{2} \frac{N!}{(LM)^N} \right] < \frac{\delta}{4}. \quad (\text{SD1})$$

The MBCS oracle only knows A but has no information whatsoever about which sample \mathfrak{S}^* has been chosen from $G_{M,N} \otimes \Omega_{L,N}$. Thus, Eq. (SD1) implies

$$\Pr_{X,A} \left[\Delta_{\mathfrak{S}^*} > \frac{\varepsilon}{2} \frac{N!}{(LM)^N} \right] < \frac{\delta}{4}. \quad (\text{SD2})$$

2. As shown in step 3 of the proof of Theorem 4, we can apply Stockmeyer's algorithm [S2] to find an approximate $\tilde{q}_{\mathfrak{S}^*}$ of $q_{\mathfrak{S}^*}$ in $\text{FBPP}^{\text{NP}^{\mathcal{O}_R}}$. The algorithm guarantees that, for an arbitrary $\alpha > 0$ and a runtime polynomial in $1/\alpha$ and M ,

$$\Pr[|\tilde{q}_{\mathfrak{S}^*} - q_{\mathfrak{S}^*}| > \alpha q_{\mathfrak{S}^*}] \leq \Pr[\tilde{q}_{\mathfrak{S}^*} > (1+\alpha)q_{\mathfrak{S}^*} \vee \tilde{q}_{\mathfrak{S}^*} < q_{\mathfrak{S}^*}/(1+\alpha)] < \frac{1}{2^M},$$

where the first inequality follows from $1 - \alpha < 1/(1+\alpha)$ and the second inequality is equivalent to Ineq. (S15). With the choice $\alpha = \varepsilon\delta/16$, this becomes

$$\Pr[|\tilde{q}_{\mathfrak{S}^*} - q_{\mathfrak{S}^*}| > \frac{\varepsilon\delta}{16} q_{\mathfrak{S}^*}] < \frac{1}{2^M}. \quad (\text{SD3})$$

3. Lastly,

$$\mathbb{E}_{\mathfrak{S} \in G_{M,N} \otimes \Omega_{L,N}}[q_{\mathfrak{S}}] = \frac{\sum_{\mathfrak{S} \in G_{M,N} \otimes \Omega_{L,N}} q_{\mathfrak{S}}}{|G_{M,N}| |\Omega_{L,N}|} \leq \frac{1}{|G_{M,N}| |\Omega_{L,N}|} = \frac{1}{\binom{M}{N} L^N} < 2 \frac{N!}{(LM)^N}$$

and thus by invoking Markov's inequality

$$\Pr_{\mathfrak{S} \in G_{M,N} \otimes \Omega_{L,N}} \left[q_{\mathfrak{S}} > 2 \frac{N!}{(LM)^2} \frac{4}{\delta} \right] < \frac{\delta}{4}.$$

With the same arguments leading to Ineq. (SD2), this implies

$$\Pr_{X,A} \left[q_{\mathfrak{S}^*} > 2 \frac{N!}{(LM)^2} \frac{4}{\delta} \right] < \frac{\delta}{4}. \quad (\text{SD4})$$

Indeed, by using the inequalities

$$\Pr[|a - b| > c] \leq \Pr\left[|a| > \frac{c}{2}\right] + \Pr\left[|b| > \frac{c}{2}\right] \quad (c > 0) \quad (\text{SD5})$$

and

$$\Pr[|a - b| > c] \leq \Pr\left[b > \frac{c}{k}\right] + \Pr[|a - b| > kb] \quad (c, k > 0), \quad (\text{SD6})$$

demonstrated in App. E, we obtain

$$\begin{aligned} \Pr\left[|\tilde{q}_{\mathfrak{S}^*} - p_{\mathfrak{S}^*}| > \varepsilon \frac{N!}{(LM)^N}\right] &\leq \Pr\left[|\tilde{q}_{\mathfrak{S}^*} - q_{\mathfrak{S}^*}| > \frac{\varepsilon}{2} \frac{N!}{(LM)^N}\right] + \Pr\left[|q_{\mathfrak{S}^*} - p_{\mathfrak{S}^*}| > \frac{\varepsilon}{2} \frac{N!}{(LM)^N}\right] \\ &\leq \Pr_{X,A}\left[q_{\mathfrak{S}^*} > \frac{8}{\delta} \frac{N!}{(LM)^N}\right] + \Pr\left[|\tilde{q}_{\mathfrak{S}^*} - q_{\mathfrak{S}^*}| > \frac{\varepsilon\delta}{16} q_{\mathfrak{S}^*}\right] + \Pr_{X,A}\left[\Delta_{\mathfrak{S}^*} > \frac{\varepsilon}{2} \frac{N!}{(LM)^N}\right] \\ &< \frac{\delta}{4} + \frac{1}{2^M} + \frac{\delta}{4} = \frac{\delta}{2} + \frac{1}{2^M}, \end{aligned}$$

where in the last step, we inserted Ineqs. (SD2), (SD3), and (SD4). This inequality is equivalent to Ineq. (S16), as can be seen by inserting the expression for $p_{\mathfrak{S}^*}$ from Eq. (S14).

Appendix E: Inequalities for probabilities

Here, we want to prove the inequalities (SD5) and (SD6).

Proof. First, observe that

$$|a| \leq \frac{c}{2} \wedge |b| \leq \frac{c}{2} \Rightarrow |a - b| \leq c$$

and therefore

$$\Pr\left[|a| \leq \frac{c}{2} \wedge |b| \leq \frac{c}{2}\right] \leq \Pr[|a - b| \leq c]. \quad (\text{SE1})$$

Second, for two events A and B , we know that

$$\Pr[A \cap B] = \Pr[A] + \Pr[B] - \Pr[A \cup B]$$

and it follows that (\bar{A}, \bar{B} denote the complement of A, B)

$$1 - \Pr[A \cap B] = 1 - \Pr[A] - \Pr[B] + \Pr[A \cup B] \leq 2 - \Pr[A] - \Pr[B] = \Pr[\bar{A}] + \Pr[\bar{B}]. \quad (\text{SE2})$$

Now, Ineq. (SD5) follows as

$$\Pr[|a - b| > c] = 1 - \Pr[|a - b| \leq c] \leq 1 - \Pr\left[|a| \leq \frac{c}{2} \wedge |b| \leq \frac{c}{2}\right] \leq \Pr\left[|a| > \frac{c}{2}\right] + \Pr\left[|b| > \frac{c}{2}\right],$$

where we used Ineq. (SE1) and Ineq. (SE2) in the second and third step, respectively.

Ineq. (SD6) can be proved in a similar way. ■

-
- [S1] S. Aaronson and A. Arkhipov, in *Proceedings of the 43rd annual ACM symposium on Theory of computing* (ACM, 2011) pp. 333–342.
[S2] L. Stockmeyer, in *Proceedings of the Fifteenth Annual ACM Symposium on Theory of Computing*, STOC '83 (ACM, New York, NY, USA, 1983) pp. 118–126.
[S3] S. Toda, *SIAM J. Comput.* **20**, 865 (1991).
[S4] This possibility was brought to our attention by S. Aaronson in a private communication.
[S5] G. Kuperberg, *Theory of Computing* **11**, 183 (2015).